

KOH

JCC/GDB: USAO 2018R00597

FILED
LOGGED
ENTERED
RECEIVED

MAY 22 2019

AT GREENBELT
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND

BY

DEPUTY

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

OSAKWE ISMAEL OSAGBUE,

Defendant

CRIMINAL NO.

UNDER SEAL

19-1816TJS

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT

I, Jeffrey Starnes, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a U.S. Postal Inspector with the U.S. Postal Inspection Service (USPIS) and have been so employed since June 2016. Prior to my employment with the USPIS, I was a Special Agent with the U.S. Secret Service (USSS) for 10 years.
2. In my capacity as a United States Postal Inspector, I investigate allegations of criminal fraud involving the use of the United States Mail. Pursuant to my duties as a U.S. Postal Inspector and previously as a USSS Special Agent, I have gained experience in investigations of mail fraud, wire fraud, bank fraud, identity theft, investment fraud, credit card fraud, counterfeit securities and currency, false identification documents, and mortgage fraud. I have participated in search and seizure operations dealing with the aforementioned types of criminal offenses.
3. This affidavit is submitted in support of a criminal complaint and arrest warrant for **OSAKWE ISMAEL OSAGBUE** ("OSAGBUE"). Based on the facts set forth in this affidavit, I submit there is probable cause to believe that **OSAGBUE** violated Title 18, United

States Code, Sections 1341 (mail fraud). I respectfully request that the Court issue an arrest warrant for **OSAGBUE** under Federal Rule of Criminal Procedure 4(a).

4. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. I have also received information from other individuals who have knowledge of the circumstances relating to this investigation, to include other law enforcement personnel. The information set forth in this affidavit is based on my own observations and review of documents, or reliable information provided to me by others. I am setting forth only those facts and circumstances necessary to establish probable cause for the issuance of the requested arrest warrant and complaint. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

STATEMENT OF PROBABLE CAUSE

Overview of the Investigation

5. As further discussed below, I have been engaged in an investigation of a fraudulent scheme in which an individual, identified as **OSAGBUE**, conducted fraudulent credit card charges using Square, Inc. (“Square”) mobile point of sale (“POS”) terminals, called Square tokens. I respectfully submit that there is probable cause to believe that, between at least in or about December 2016 and at least in or about December 2018, **OSAGBUE** engaged in this fraudulent scheme by conducting fraudulent transactions using JP Morgan Chase (“Chase”) payment cards on Square tokens and that Chase cards were sent through the mails – specifically,

through the United Parcel Service (“UPS”) – to the District of Maryland in furtherance of this fraudulent scheme.

Background Information

6. It is common knowledge that financial institutions issue payment cards, such as credit and debit cards, to accountholders for their legitimate use in accessing the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of the financial institution. These payment cards contain a magnetic strip or chip that stores account data, such as the payment card number and any associated personal identification number, security code, or expiration date. Among other uses, payment cards can be used at various retail locations to make purchases.

7. It is also widely known that POS terminals allow for retailers to electronically conduct legitimate payment card transactions, by reading the magnetic strip or chip as the payment card is either swiped or inserted through the POS terminal. Mobile POS terminals allow for the processing of the payment card transactions through a device and application that can be attached and downloaded to a mobile device, such as a smartphone or tablet.

8. Square is a merchant services provider marketing mobile POS software (the Square application) and hardware (Square tokens) to merchants. The merchants contract with Square, download the Square application, and receive a corresponding Square token. The Square token is a physical magnetic strip or chip reader that the merchant can plug into their mobile device, such as a phone or tablet, connecting to the Square application. The Square token can then be used as a conventional POS terminal that payment cards can be swiped through or inserted into in order to conduct transactions. Internet service is required throughout the transaction.

9. A single Square token can be used by multiple merchants. In order to do this, an individual merely needs to access the Square application on their mobile device or tablet, log out of the account for one merchant, and log into the account for another merchant. This feature is intended for individuals who own multiple businesses, allowing them to only purchase one Square token. Therefore, each Square token can easily be used by multiple merchants, or the same individual with multiple accounts. Further, like purchases made using conventional POS terminals, a Square token is linked with a bank account to receive the proceeds of the transaction. Each Square token can only be linked to a single bank account at one time, even if that token may be used by multiple merchants.

The Fraudulent Scheme

10. On or about May 30, 2018, Chase contacted agents with the USSS and USPIS regarding fraudulent charges made on Chase payment cards. Specifically, Chase reported, among other transactions, approximately \$1,800,000 (\$1.8 million) in fraudulent transactions, occurring between December 2016 and June 2018, using Square tokens as mobile POS terminals, from approximately 150 different merchants using over 90 different Chase-issued payment cards. Additionally, Chase reported that for each of the payment cards involved, a replacement card had been fraudulently ordered and delivered to unknown individuals. Chase reported the fraudulent transactions were made using these replacement cards.

11. On or about June 20, 2018, agents with the USSS and USPIS contacted Square regarding the potentially fraudulent transactions made using Square mobile POS terminal services. Square confirmed that while the fraudulent transactions appeared to be conducted by approximately 130 of the 150 different merchants initially reported by Chase, only four Square tokens were used. As noted above, each Square token can be used by multiple merchants, or the

same individual with multiple accounts. Square confirmed that 46 of the merchants conducted transactions using Square token 8ES9W4KZT6MX0; 45 used Square token 9TGVK5S8D3Z7Z; 43 used Square token FSBJGWJ0NNM43; and 3 used Square token KKCHTWVTGXW5P.

12. Based on records provided by Chase, there were approximately \$1,300,000 (\$1.3 million) in fraudulent purchases made using these four specific Square tokens.

13. During the course of their investigation, Chase contacted a number of the identity theft victims whose information had been used to set up the bank accounts. These victims confirmed that they never applied for a Chase credit card and did not know that an account had ever been opened in their names. It was determined that while the victims lived throughout the country, the vast majority of the replacement credit cards were delivered by UPS to addresses in Maryland.

14. Generally, each Square token captures the GPS results for each transaction, showing the location where the transaction took place. However, Square confirmed the GPS results for each of the four tokens listed above were being altered by the user to match the general location (e.g., Pacific Northwest) of each merchant.

15. The following are examples of merchant names used in this scheme for each of the Square tokens identified:

Square Token	Merchant Name	Merchant Location
FSBJGWJ0NNM43	Davinci Plastic Surgery	Washington, D.C.
8ES9W4KZT6MX0	Salmon Creek Plastic Surgery	Vancouver, WA
9TGVK5S8D3Z7Z	Naficy Plastic Surgery	Bellevue, WA
KKCHTVWTGXW5P	Newvue Plastic Surgery	Bellevue, WA

16. Square confirmed that each of the above-described Square tokens was linked to a Bank of America (BOA) account, as described below:

a. Square Token FSBJGWJ0NM43 has been linked to three different BOA accounts, although it has only been linked to a single bank account at any one time:

i. Square token FSBJGWJ0NM43 was linked to BOA account ending in 3795, which was opened on or about February 21, 2018. BOA account ending in 3795 is registered to 3D Construction Services Inc. with Aurora Kirbo as the account owner. 3D Construction Services Inc. was incorporated in the state of Georgia on June 2, 2017, with the registered agent and incorporator being Steve Randal Davis Jr., and the director, CEO, CFO, and Secretary being Aurora Kirbo.

ii. Square token FSBJGWJ0NNM43 was also linked to BOA account ending in 5386, which was opened on or about February 20, 2018. BOA account ending in 5386 is registered to A Construction Inc. with Coleen Keenan as the account owner. A Construction Inc. was incorporated in the state of Georgia on April 20, 2006, with Alejandro Martinez as the owner and incorporator.

iii. Square token FSBJGWJ0NNM43 was also linked to BOA account ending in 4537, which was opened on or about January 19, 2017. BOA account ending in 4537 is registered to 3D Concrete Construction, Inc. with David Meador as the account owner. 3D Concrete Construction, Inc. was incorporated in the state of Georgia on June 10, 2013, with Stephen Washkill Jr. as the incorporator and Crystal Washkill as the owner.

b. Square token 9TG VK5S8D3Z7Z was linked to BOA account ending in 7431, which was opened on or about January 19, 2017. BOA account ending in 7431 is registered to A&E Concrete Construction, Inc., with James Pannell as the account owner. A&E Concrete Construction, Inc. was incorporated in Georgia on October 10, 2003, with Timothy Hill as the incorporator.

c. Square token 8ES9W4KZT6MX0 was linked to BOA account ending in 4446, which was opened on or about January 19, 2017. Additionally BOA account ending in 4446 is registered to 12th Man Construction Inc., with Dwan Smith as the account owner. 12th Man Construction Inc., was incorporated in the state of Georgia on February 9, 2016, with Austin Perdeiu as the incorporator and Dwan Smith as CEO, CFO, and Secretary.

d. Square token KKCHTVWTGXW5P was linked to BOA account ending in 3803, which was opened on or about February 21, 2018. BOA account ending in 3803 is registered to 3D Construction Services Inc., with Aurora Kirbo as the account owner. 3D Construction Services Inc. was incorporated in the state of Georgia on June 2, 2017, with the registered agent and incorporator being Steve Randal Davis Jr., and the director, CEO, CFO, and Secretary being Aurora Kirbo.

17. As reflected above, the business names provided to open the business accounts with BOA do not match the merchant names associated with the corresponding Square tokens. For instance, proceeds from the Square token associated with merchant name Davinci Plastic Surgery were deposited into BOA accounts ending in 4537 (opened using business name 3D Concrete Construction, Inc.) and 5386 (opened using business name A Construction Inc.). Proceeds from the Square token associated with merchant name Salmon Creek Plastic Surgery were deposited into BOA account ending in 4446 (opened using business name 12th Man Construction Inc.). Proceeds from the Square token associated with merchant name Naficy Plastic Surgery were deposited into BOA account ending in 7431 (opened using business name A&E Concrete Construction, Inc.). Proceeds from the Square token associated with merchant name Newvue Plastic Surgery were deposited into BOA account ending in 3803 (opened using business name 3D Construction Services Inc.).

Use of the Home Internet Account and Identification of OSAGBUE

18. A new Square token, 88JER7P9K0N16, was identified by Square in December 2018 as being connected to one of the four original Square tokens, FSBJGWJ0NNM43. Square connected the two tokens via browser information and believes the same device was used to log into merchant accounts for both tokens. Two fraudulent transactions were conducted using token 88JER7P9K0N16 prior to Square identifying and disabling the token. The two fraudulent transactions were conducted using a Chase card.

19. Chase confirmed both transactions were not authorized and thus fraudulent. As with the four original Square tokens, Square confirmed that the GPS results for the transactions associated with Square token 88JER7P9K0N16 were altered by the user to match the geographical region of the merchant. In this case, the GPS location information for the fraudulent transactions completed using Square token 88JER7P9K0N16 falsely indicated that the token was being used in Wisconsin. However, the IP addresses accessed by Square token 88JER7P9K0N16 at the time of the fraudulent transactions showed that the token was in California.

20. Square token 88JER7P9K0N16 is linked to BOA account ending in 2380, which was opened on or about August 14, 2018. BOA account ending in 2380 is registered to MVE Automobile Financial Co. Inc. with Soraya James as the account owner. MVE Automobile Financial Co. Inc. was incorporated in the state of Georgia on May 1, 2018, with the registered agent being Abdua Kkkyha, and the incorporator being Claud McIver.

21. One of the transactions on Square token 88JER7P9K0N16 occurred on or about November 28, 2018 at or around 11:56 p.m. Square identified an IP address of 76.169.58.84 that accessed the token at that date and time. The IP address (76.169.58.84) belongs to the internet service provider Spectrum, which is owned by Charter Communications, Inc.

22. According to records from Charter Communications, at the time of the November 28 transaction, the IP address 76.169.58.84 belonged to a residential internet account for 4510 Murietta Avenue, Unit 203, Sherman Oaks, CA 91423. The records identified the owner of this internet account as **OSAGBUE**, and identified the phone number associated with this internet account as 240-779-3559 (the "3559 Number").

23. Information was obtained in February 2019 from the Los Angeles Department of Water and Power (LADWP) in response to an inquiry regarding the 4510 Murietta Avenue address. According to this information, LADWP records showed the utility bill in the name **OSAGBUE**. Additionally, the phone number associated with the LADWP utility account was the 3559 Number.

24. Records from T-Mobile indicate the subscriber of the 3559 Number is "Osakwe I Osag," with an address of 2070 Cobblestone Cir. NE, Brookhaven, GA 30319. **OSAGBUE**'s Georgia driver's license lists his address as the above-mentioned 2070 Cobblestone address. Additionally, T-Mobile provided the date of birth and social security number of the subscriber, both of which match the date of birth and social security number of **OSAGBUE**.

25. The 3559 Number was compared to records provided by Chase of phone numbers that called Chase regarding the fraudulently obtained cards described above. The 3559 Number was identified calling Chase regarding six of the fraudulently obtained cards between the dates of November 5, 2017 and December 21, 2017.

26. According to Chase records, the fraudulent charges for these six cards alone total \$116,348.72. Of the 28 fraudulent charges conducted using these six cards, 25 were transactions conducted using three of the original four Square tokens (tokens 8ES9W4KZT6MX0, 9TGVK5S8D3Z7Z, and FSBJGWJ0NNM43).

27. Each of these six cards were shipped via UPS and delivered to the addresses listed below:

Date delivered	Last Four of Card Number	Address of Card Delivery
8/15/2017	1636	7006 Emerson Street, Hyattsville, MD 20784
11/8/2017	7330	7515 Annapolis Road, Hyattsville, MD 20784
11/9/2017	9941	4610 69 th Avenue, Hyattsville, MD 20784
11/9/2017	1772	4610 69 th Avenue, Hyattsville, MD 20784
8/15/2017	3764	4102 73 rd Avenue, Hyattsville, MD 20784
8/16/2017	5962	3908 71 st Avenue, Hyattsville, MD 20784

28. For example, the Chase card ending in 3764 was delivered by UPS on or about August 15, 2017 to 4102 73rd Avenue, Hyattsville, MD 20784. According to Chase records, there was one fraudulent charge on the card, on or about September 22, 2017, for \$4,625.18 conducted using Square token 9TG VK5S8D3Z7Z under the merchant name Naficy Plastic Surgery. The 3559 Number was used to call Chase regarding the account for Chase card ending in 3764 on or about November 5, 2017. On or about the same day, the same phone number was used to call Chase regarding the accounts for cards ending in 5962 and 1636.

29. According to Chase records, the account for Chase card ending in 3764 was initially opened on February 17, 2016 using Victim 1's name, with a street address in Phoenix, MD.

30. On April 29, 2019, I spoke to Victim 1 by telephone. Victim 1 stated he has never had accounts with Chase, credit cards or otherwise, and was not aware that any Chase accounts were ever opened in his name.

31. Driver's license photographs were obtained for **OSAGBUE** for licenses in Maryland and Georgia. The address listed on **OSAGBUE**'s Maryland license is 6916 Annapolis Road, Hyattsville, MD 20784. The 6916 Annapolis Road address is owned by an individual believed to be the father of **OSAGBUE** and has been so owned since 1994.

32. As noted above, the majority of the fraudulently obtained Chase cards were mailed to addresses in Maryland. Of those cards mailed to addresses in Maryland, the vast majority were mailed to various addresses in the same 20784 zip code as **OSAGBUE**'s Maryland address. In fact, many were mailed to various addresses on Annapolis Road within walking distance of **OSAGBUE**'s Maryland address, as well as to other addresses within one mile of the residence. For example, according to Google Maps, 4102 73rd Avenue, Hyattsville, MD 20784 – the address to which Chase card ending in 3764 was delivered – is located approximately 0.7 miles (walking) from **OSAGBUE**'s Maryland address.

33. **OSAGBUE** also has a license in Georgia with an address in the Atlanta area, 2070 Cobblestone Circle NE, Brookhaven, GA 30319. As described above, according to T-Mobile records, the 2070 Cobblestone Circle NE address is the address on the account for the subscriber of the 3559 Number. In addition, as detailed above, the addresses listed on the BOA accounts, as well as the addresses for the corresponding business registrations, are located in Georgia.

Bank Surveillance Photographs

34. Bank surveillance photographs provided by BOA from various BOA branches in Maryland, Georgia, and Southern California show an individual conducting account transactions with the BOA accounts linked to the Square tokens involved in the fraudulent scheme, as described above, between March 7, 2018 and July 3, 2018. The individual's face is partially obscured by a hat in these photographs. The transactions are detailed below:

Date	Branch city, state	Business name on account
3/7/2018	Tarzana, CA	3D Concrete Construction, Inc.
3/12/2018	Sun Valley, CA	A Construction, Inc.
3/18/2018	Tarzana, CA	A & E Concrete Construction, Inc.
3/21/2018	Atlanta, GA	A & E Concrete Construction, Inc.
4/26/2018	Stockbridge, GA	A & E Concrete Construction, Inc.
4/25/2018	Atlanta, GA	A & E Concrete Construction, Inc.
6/12/2018	Tucker, GA	3D Construction Services Inc.
6/13/2018	Chamblee, GA	3D Construction Services Inc.
6/19/2018	Greenbelt, MD	12th Man Construction Inc.
6/26/2018	Woodland Hills, CA	12th Man Construction Inc.
7/3/2018	Atlanta, GA	3D Construction Services Inc.

35. **OSAGBUE** was arrested on September 3, 2018 by the Brookhaven Police Department on an outstanding warrant for failure to appear on a DUI charge. At that time, **OSAGBUE** was taken into custody outside of the Cobblestone Circle NE address listed on his Georgia driver's license. The arrest report identifies **OSAGBUE**'s phone number as the 3559 Number.

36. Body camera footage was obtained of the arrest. The footage shows **OSAGBUE** walking up the steps to the residence when verbal contact was made by the initial arresting officer.

37. A review of the body camera footage shows **OSAGBUE** wearing a black t-shirt with the word "Dream" on it and camouflage shorts. **OSAGBUE** was also wearing a watch, gold in color, on his left wrist; a ring, light in color, on his right middle finger; and a neck chain, light in color, around his neck. Officers found a black wallet in **OSAGBUE**'s pocket as well as a wad of money with a \$50 bill on the outside. The wad of money had a purple band on it that appeared to read \$2,000. A Chase Bank card can be seen in the wallet when the officer briefly opens it up during the arrest.

38. The body camera footage of **OSAGBUE**'s arrest, as well as **OSAGBUE**'s driver's license photographs, were compared to the surveillance pictures from BOA for the transactions

conducted between March 7, 2018 and July 3, 2018. Based on this comparison, the individual in the surveillance photographs appears to be **OSAGBUE**. Additionally, the watch and neck chain worn by **OSAGBUE** in the arrest footage appears to be consistent with jewelry worn by the individual in the BOA bank surveillance pictures from March 7, 2018 (watch and neck chain) and June 26, 2018 (neck chain).

39. BOA also provided video footage of cash withdrawal transactions from BOA account ending in 2380 that occurred on or about November 29, 2018, November 30, 2018, December 4, 2018, December 5, 2018, and December 7, 2018. As described above, BOA account ending in 2380 was linked to Square token 88JER7P9K0N16, which was used to conduct fraudulent transactions in or around November 2018. The cash withdrawals^{al} that occurred on or about November 29, 2018, November 30, 2018, December 4, 2018, and December 7, 2018 were conducted at a BOA branch in North Hollywood, CA. The transaction that occurred on or about December 5, 2018 was conducted at a BOA branch in Northridge, CA.

40. The face of the individual conducting these transactions is partially obscured by a hat in all of these videos. However, based on a comparison to body camera footage of **OSAGBUE**'s arrest, as well as **OSAGBUE**'s driver's license photographs, the individual appears to be **OSAGBUE**. In the transactions on November 29, 2018, December 5, 2018, and December 7, 2018, the individual conducting the transactions is wearing a black sweatshirt with the word "HIGHER" on it in green lettering.

41. **OSAGBUE** also maintains a personal Chase bank account (account number ending in 2729) under his own name. The phone number provided for the account is the 3559 Number. Chase provided bank surveillance images of the following transactions for this account: a \$2,000 cash deposit at a Chase branch in Atlanta, GA on or about September 4, 2018;

a \$3,400 cash deposit at the same Chase branch in Atlanta, GA on or about September 18, 2018; and a \$1,660 cash deposit at a Chase branch in Sherman Oaks, CA on or about December 5, 2018. The individual in the images is **OSAGBUE**. He is not wearing a hat while conducting transactions on his personal account.

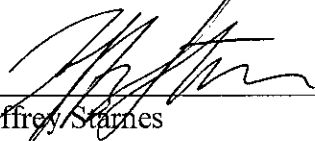
42. Both Chase and BOA provided surveillance video or images for transactions occurring on December 5, 2018. Specifically, a cash withdrawal from BOA account ending in 2380 for \$1,700 occurred at approximately 9:52 a.m. Pacific Time on that date. In addition, a cash deposit into **OSAGBUE**'s personal Chase account for \$1,660 occurred at approximately 10:38 a.m. Pacific Time. The Chase images show that, during the cash deposit into his personal account, **OSAGBUE** was wearing a black sweatshirt with the word "HIGHER" on it in green lettering, matching the sweatshirt seen in the BOA surveillance video from that date. The BOA branch and Chase branch are approximately 8.5 miles apart via car according to Google Maps. As described above, the individual in the BOA surveillance videos appears to be wearing the same sweatshirt during the November 29, 2018 and December 7, 2018 cash withdrawals.

Conclusion

43. Based on the facts set forth herein, I respectfully submit that there is probable cause to believe that, on or about August 15, 2017, **OSAGBUE** violated Title 18, United States Code,

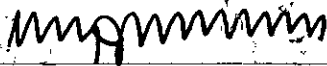
Sections 1341 (mail fraud). Therefore, I request the issuance of a criminal complaint and an arrest warrant.

Respectfully submitted,



Jeffrey Starnes
Postal Inspector
United States Postal Inspection Service

Subscribed and sworn to before me on this 22nd day of May, 2019.



HON. TIMOTHY J. SULLIVAN
UNITED STATES MAGISTRATE JUDGE